Manual de usuario del entorno admin. Iván Roldán

1.Acceso al entorno de administración....2
2.Login....3
3.Funcionamiento de la intranet....4
3.1.Registro de un nuevo usuario....4
3.2.Menú lateral....6
3.3.Opciones de la sección central de la intranet....8
3.3.1.Opciones para el servidor proxy squid....8
3.3.1.1.Edición de archivos....8
3.1.1.2.Monitorizar Squid....13
3.1.1.3.Restaurar archivos....14
3.1.1.4.Reinicio del servicio....14
3.1.2.Opciones para el firewall Shorewall/Iptables....15
3.1.2.1.Edición de archivos....15
3.1.2.2.Monitorizar el Firewall....21
3.1.2.3.Restauración de archivos....22
3.1.2.4.Reinicio del servicio....23

1.Acceso al entorno de administración.

El acceso al entorno se realiza mediante la URL:

```
http://profire.iesebre.com
```

Tan solo se permitirá el acceso desde las direcciones IP de los profesores o bien desde la propia máquina local.

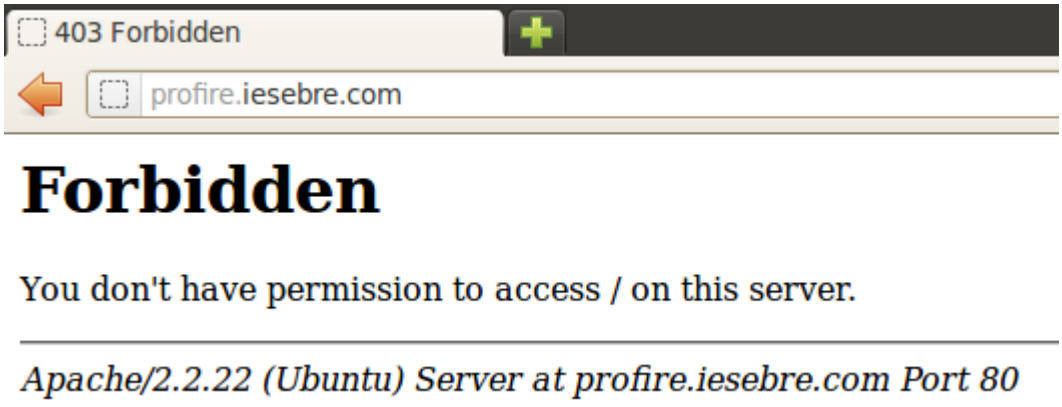
-192.168.202.100

-192.168.203.100

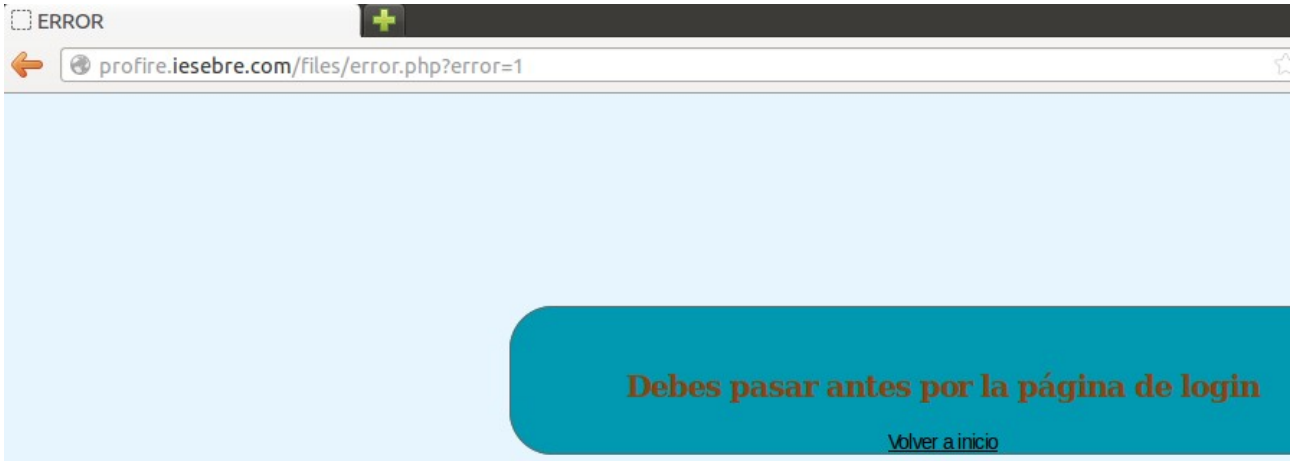
-192.168.204.100

-localhost

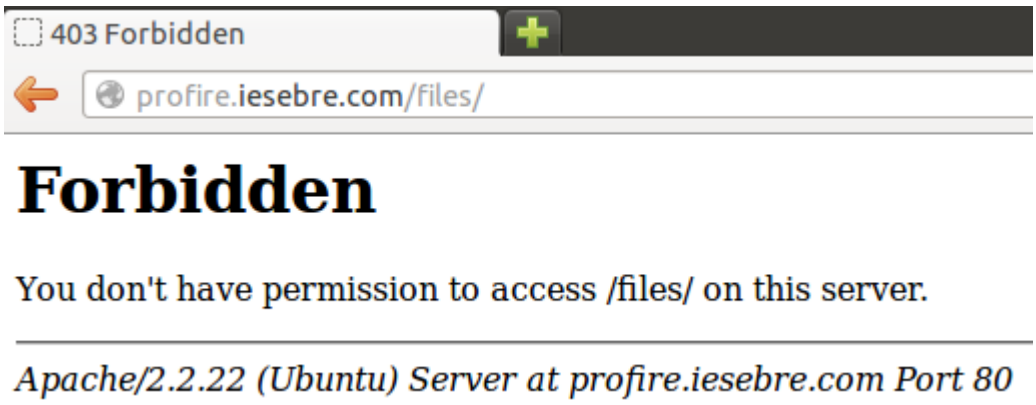
Sin intentásemos el acceso desde una dirección IP que no fuera una de las autorizadas, nos encontraremos el correspondiente mensaje de error.


403 Forbidden
profire.iesebre.com
Forbidden
You don't have permission to access / on this server.
Apache/2.2.22 (Ubuntu) Server at profire.iesebre.com Port 80

De igual manera tampoco se podrá intentar acceder a las zonas de la intranet,registrar usuarios nuevos o bien a la página de validación de usuarios a través de la URL sin haber pasado por la página de login, pues se nos mostrará un mensaje de aviso

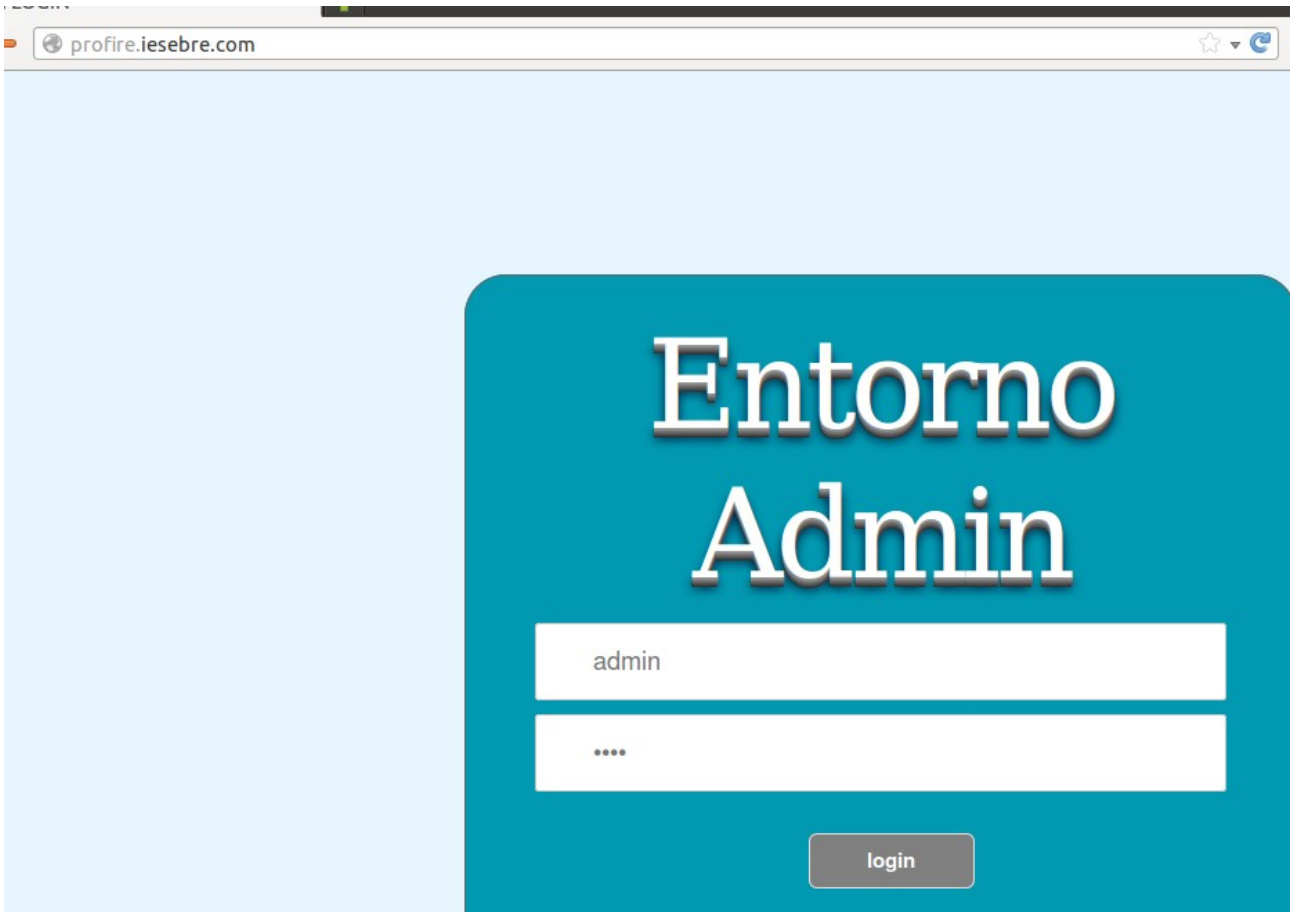


El servidor está configurado de manera que en aquellos directorios en los que no existe un index, no se podrá entrar.

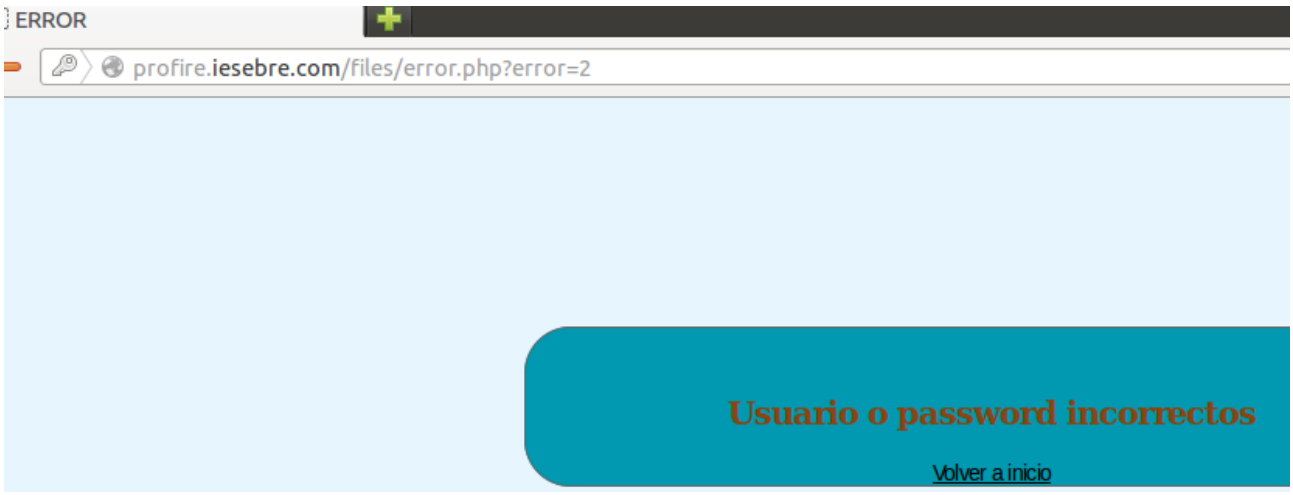

403 Forbidden
profire.iesebre.com/files/
Forbidden
You don't have permission to access /files/ on this server.
Apache/2.2.22 (Ubuntu) Server at profire.iesebre.com Port 80

2.Login.

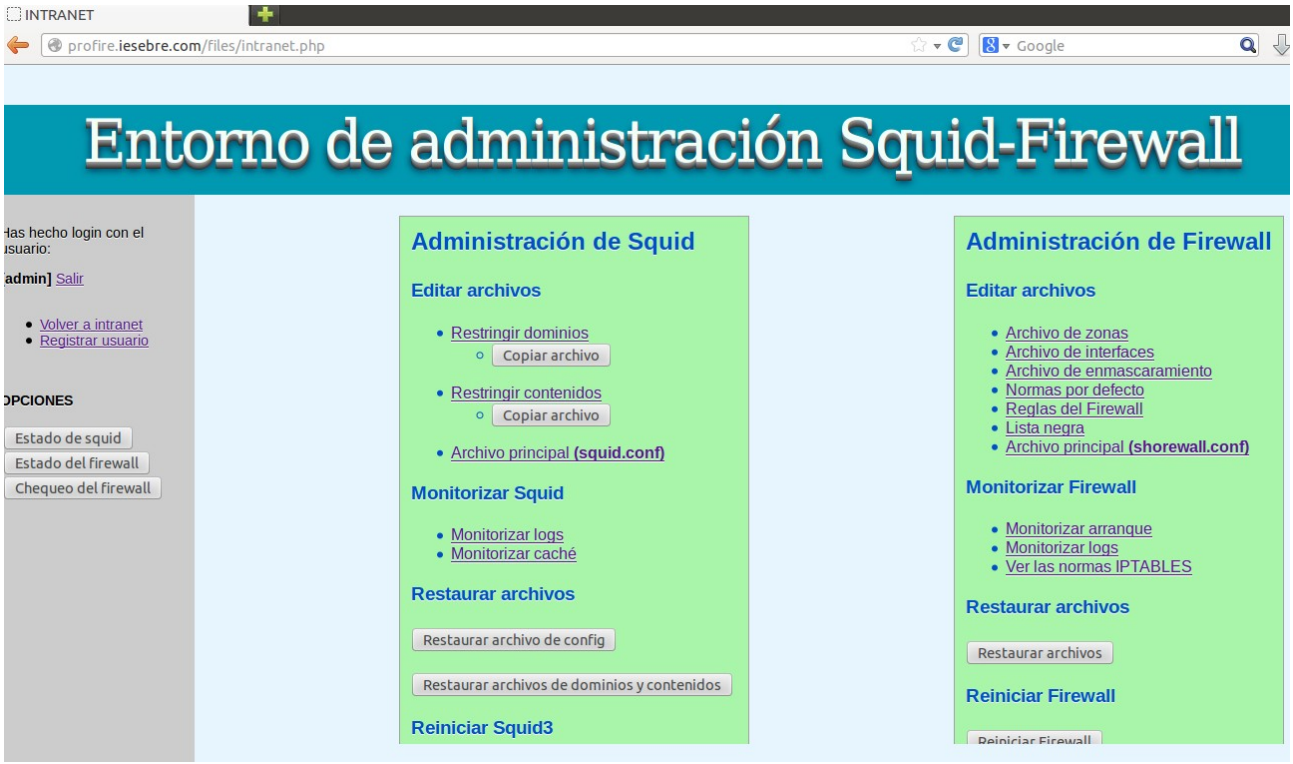
Si cumplimos todos los requisitos mencionados en el apartado anterior y accedemos a la página inicial nos encontraremos con los campos para introducir el usuario y contraseña. Lógicamente, el usuario debe existir en la base de datops para poder tener acceso.



Deberemos introducir el usuario y contraseña correctos para poder acceder a la intranet, en caso contrario nos avisará de que alguno de los campos es incorrecto.



Una vez introducidos los campos correctamente, se validarán con respecto a los existentes en la base de datos y nos permitirá el acceso a la intranet.



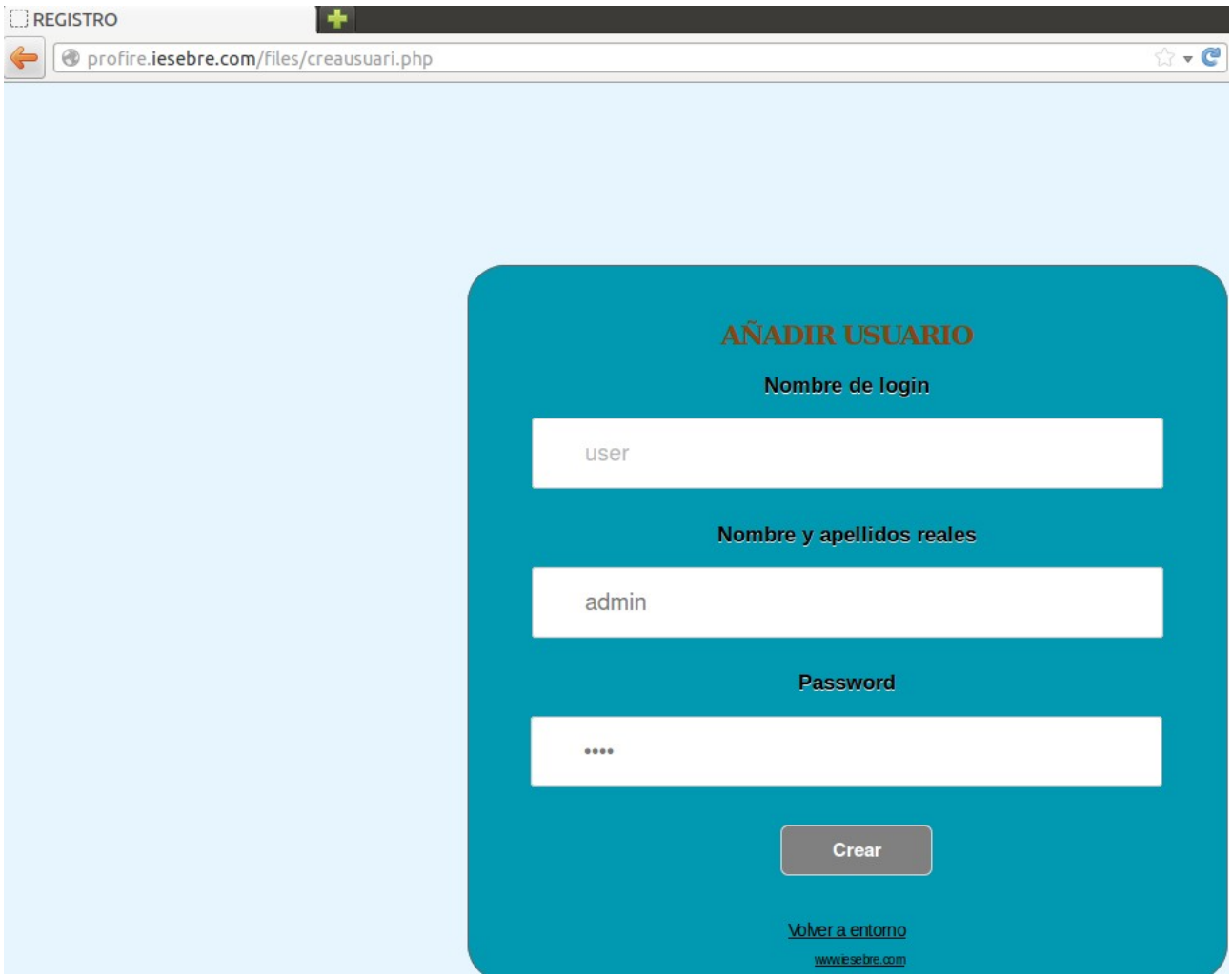
3.Funcionamiento de la intranet.

Explicaremos aquí de manera detallada el funcionamiento de la intranet y todas sus funciones.

Desde esta página podremos realizar todas las acciones requeridas en el enunciado de este proyecto.

3.1.Registro de un nuevo usuario.

En el menú lateral de la página, trás el saludo, encontraremos un enlace que nos envirá a una página donde podremos crear nuevos usuarios administradores.



Tendremos 3 campos para rellenar que son obligatorios:

Nombre de login : Este será el alías del usuario, que utilizará para poder entrar en la página de login a la intranet.

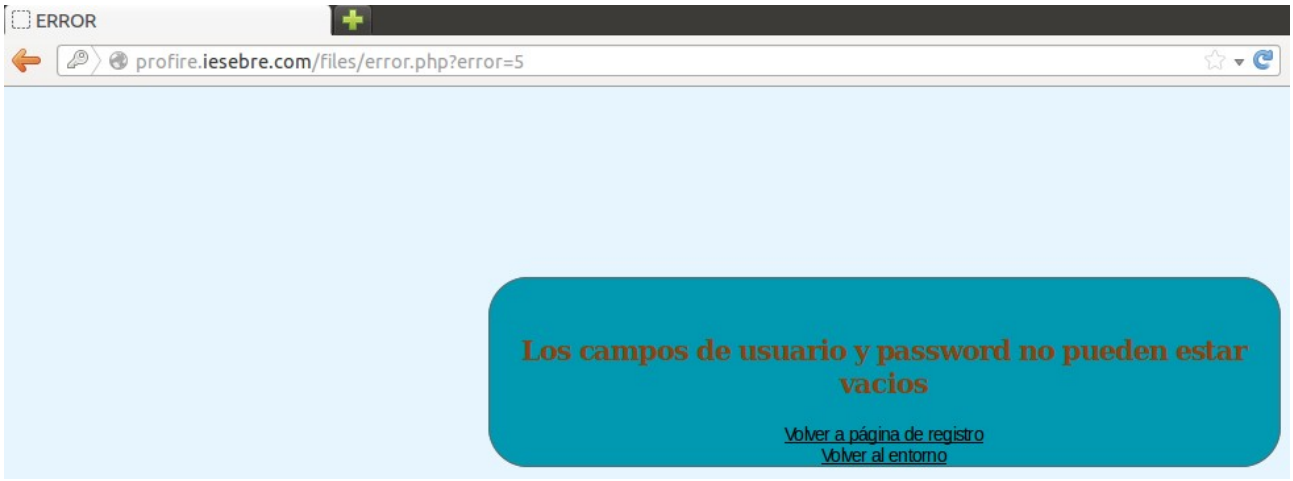
Nombre y apellidos reales : Nombre y apellidos del usuario administrador que vamos a crear.

Password : Contraseña que empleará el usuario para poder acceder a la página de la intranet.

Si se nos olvidase rellenar alguno de los campos requeridos, no se nos permitirá el envío del formulario.

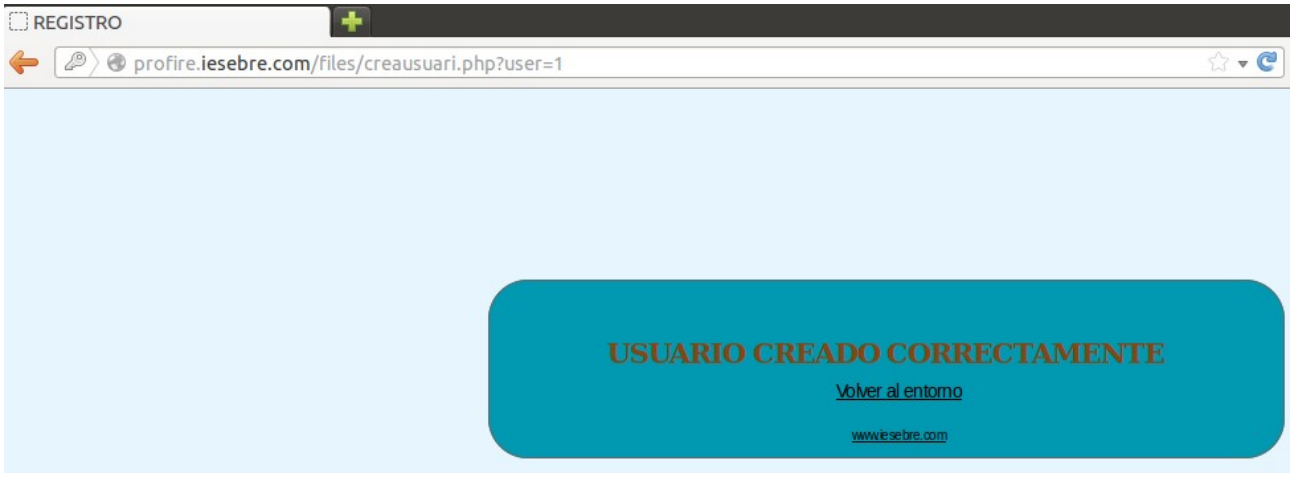
Los campos no podrán tener espacios en blanco, en el caso de introducir algún campo cuyo valor

sea un espacio en blanco, se nos dará un aviso de error.


ERROR
profire.iesebre.com/files/error.php?error=5
Los campos de usuario y password no pueden estar vacios
Volver a página de registro
Volver al entorno

Para registrar un usuario no deberemos emplear tildes o eñes pues al introducir los datos en la base de datos estos son sustituídos por caracteres y tendríamos problemas a la hora de intentar acceder a la intranet desde la página de login.

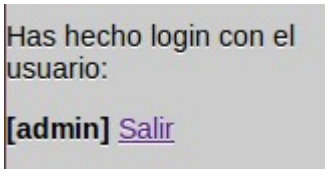
Una vez hemos rellenado los campos correctamente nos avisará de que el usuario se ha creado correctamente y podremos utilizarlo para acceder a la intranet desde la página de login.



3.2.Menú lateral.

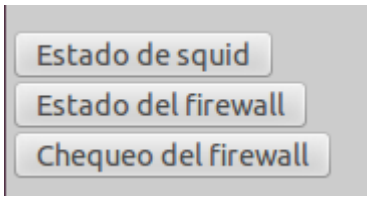
En la intranet dispondremos de un menú en lado izquierdo de la página desde el que accederemos a varias opciones.

Veremos un saludo inicial que nos dirá el usuario con el que hemos entrado en la intranet y un enlace para salir de la misma.

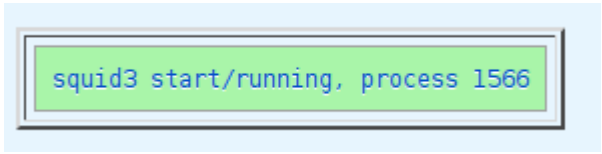


Justo debajo veremos 2 enlaces que nos permitirán volver de nuevo a la página inicial de la intranet o bien registrar un usuario nuevo.

Más abajo dispondremos de un pequeño menú de opciones que nos permitirá 3 acciones:



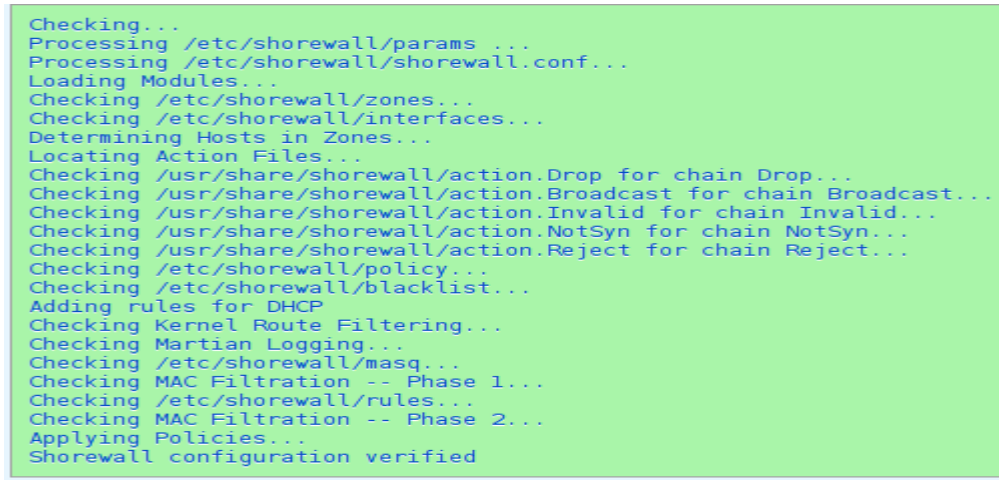
Estado de Squid : Este boton ejecuta la orden que permite visualizar el estado del servidor proxy en pantalla.



Estado del firewall : Similar al anterior, comprueba el estado del firewall y veremos el mensaje en la pantalla principal.

Shorewall-4.4.26.1 Status at server10 - Fri May 9 10:56:39 CEST 2014
Shorewall is running
State:Started (Fri May 9 08:23:24 CEST 2014) from /etc/shorewall/

Chequeo del firewall : Esta opción realizará una comprobación de la configuración del firewall, que nos mostrará en la pantalla principal.



3.3.Opciones de la sección central de la intranet.

En la pantalla central de la intranet tendremos 2 menús bien diferenciados para ejecutar todas las acciones que se solicitan en el enunciado de este proyecto tanto para el servidor proxy como para el firewall.

3.3.1.Opciones para el servidor proxy squid.

Detallaremos en este apartado todas las opciones de administración que nos ofrece el entorno sobre el servidor proxy.

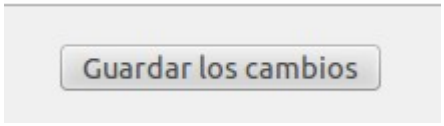
3.3.1.1.Edición de archivos.

La primera parte del menú para controlar el servidor proxy, nos permitirá la edición de los tres archivos que utiliza squid.

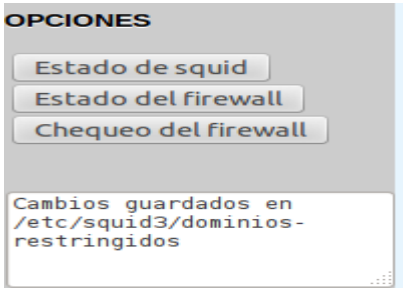
Restringir dominios : En este archivo podremos añadir una serie de dominios a los que deseamos, el servidor proxy prohiba el acceso. La forma de editarlo es tan sencilla como crear una lista. Normalmente para especificar un dominio se debe comenzar por un ' . ' y el nombre de dominio.

Ejemplo. Para prohibir el dominio marca.com escribiremos: **.marca.com**

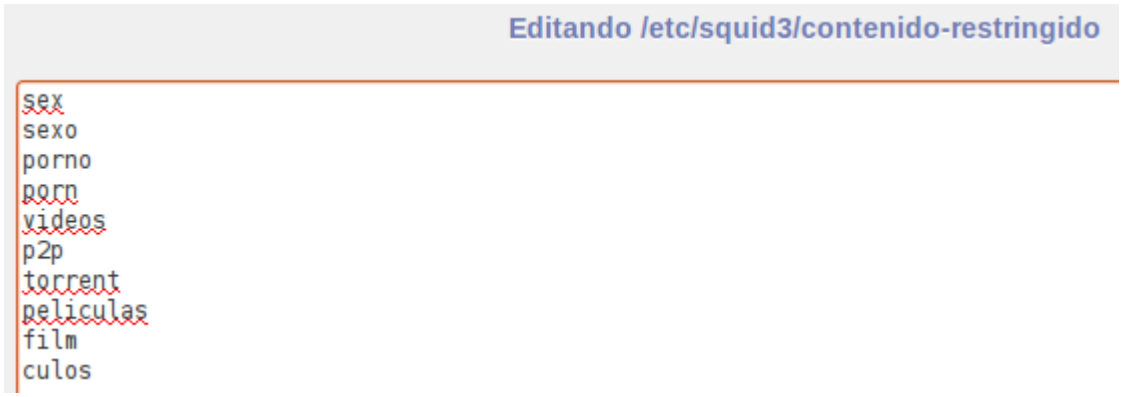
Una vez hayamos editado el archivo bastará con pulsar el botón **' Guardar los cambios '.**



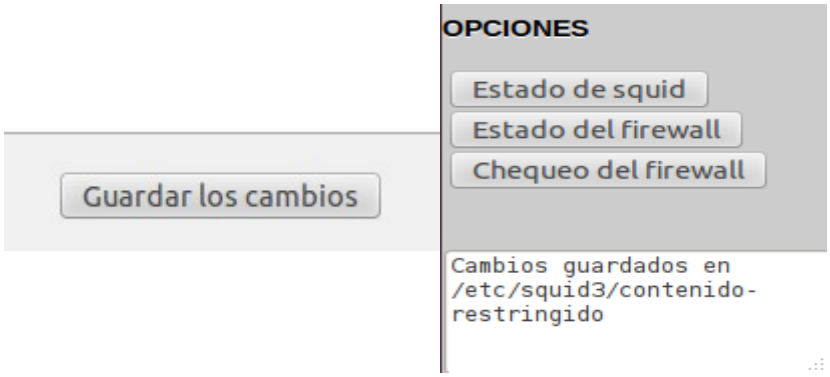
Se nos dará un aviso en el menú lateral de los cambios realizados.



Restringir contenidos : Archivo que emplearemos para filtrar los contenidos de las páginas web, por palabras. Para editarlo, como en el caso anterior deberemos ir añadiendo las palabras en forma de lista.



Una vez editado, pulsaremos el botón ' **Guardar los cambios** ' y se nos mostrará el mensaje en el menú lateral de la correcta edición.



Botón ' Copiar archivo ' : En el caso del servidor proxy, se ofrece la posibilidad de guardar una copia de los dos archivos anteriores.

Se entiende que con el paso del tiempo, se irán añadiendo nuevos dominios que se quieren restringir o bien contenidos que se quieran restringir. Si sucediese algo a esos archivos, sería tedioso tener que volver a completarlos de nuevo.

Es por esto que en la sección de editar archivos de Squid se ofrece la posibilidad de guardar una copia de cada uno de estos archivos.

De esta forma si algo sucediese, se podrían restaurar.

Se guardará una copia en el directorio /etc/squid3/copias que podrá ser restaurado en caso necesario.

Archivo principal(squid.conf): Este es el archivo principal de configuración del servidor squid. No se debería editar ni modificar, pero tal como se pide en el enunciado, el entorno de administración

nos permite hacerlo.

Encontraremos una serie de parámetros diferentes. La estructura se basa en la creación de ACLs o listas de control de acceso en las que podremos especificar diferentes parámetros y después una serie de permisos sobre estas ACL.

Además encontraremos parámetros relativos a la configuración genérica de squid.

Estructura y sintaxis de las ACL:

La sintaxis de las ACL es:

acl <nombre de acl> <parámetro> <valor>

Podremos asignarle el nombre identificativo que creamos conveniente.

En las opciones de parámetros tenemos:

src : Ips de origen

dst : Ips de destino

time : Definir días de la semana y horarios:

M : Lunes.

T: Martes.

W: Miércoles.

H: Jueves.

F: Viernes.

A: Sábado.

S: Domingo.

La hora la escribimos en formato : h1:m1-h2:m2 ==> hora de inicio y fin

url_regex [-i] : Define un patrón coincidente. -i nos sirve para las mayúsculas-minúsculas.

srcdomain : Dominio de origen

dstdomain : Dominio de destino

Ejemplos:

-ACL para una determinada red de origen.

```
acl redx src 192.168.100.0/24
```

-ACL para una determinada red de destino.

```
acl redx dst 192.168.100.0/24
```

-ACL para determinados días de la semana(Lunes-Jueves).

```
acl dias time MTWH
```

-ACL para determinados días de la semana y una franja horaria.

```
acl dias_hora time MTWH 08:00-12:00
```

-ACL para determinar un patrón coincidente.

```
acl patron url_regex -i videos
```

Podemos especificar una lista en un archivo y pasar el archivo como parámetro.

```
acl patron url_regex -i “/ruta/al/archivo”
```

-ACL para un dominio de origen.

```
acl dominio src domain .iesebre.com
```

-ACL para un dominio de destino

```
acl dominio dstdomain .iesebre.com
```

Una vez creadas las ACL deberemos permitir o denegar el acceso a las mismas con la directiva correspondiente usando el nobre que le hemos asignado a la ACL.

Estructura y sintaxis de http_access:

La sintaxis de esta directiva es la siguiente.

http_access [allow|deny] <nombre_ACL>

allow : Permitiremos el acceso al valor de dicha ACL.

Deny : Negaremos el acceso al valor de la ACL.

Ejemplos:

-Permitimos el acceso a una determinada red especificada en una ACL llamada ' red '.

```
http_access allow red
```

-Denegamos el acceso a esa red.

```
http_access deny red
```

-Permitimos el acceso a todas las redes excepto a la red de una ACL.

```
http_access allow !red
```

-Denegamos el acceso a todas las redes excepto a una determinada red.

```
http_access deny !red
```

-Permitimos el acceso a una red pero solo los días especificados en una ACL de nombre ' dias '.

```
http_access allow dias red
```

Directivas del archivo squid.conf:

El resto de directivas que encontraremos en el archivo son parámetros de configuración de squid que no deberíamos modificar.

Puerto de escucha:

```
http_port 3128
```

Caché de squid:

```
debug-options ALL,1 33,2
cache_mem 1000 MB
cache_dir ufs /var/spool/squid3 10000 16 256
```

debug-options : Opciones de depuración para la caché (/var/log/squid3/cache.log)

ALL : Quiere decir todas las secciones. Si sólo queremos depurar una sección la debemos indicar por su número. Las secciones se pueden consultar en:

```
http://www.linofee.org/~jel/proxy/Squid/debug.shtml
```

33 : Client-side Routines

cache_mem : Cantidad de memoria adicional que podrá utilizar para la caché (1GB).

cache_dir : Tipo de formato, directorio, cantidad de memoria(10GB) que podrá usar,nº de subdirectorios, nº de niveles en cada subdirectorio.

Logs de squid:

```
logformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid3/access.log squid
logfile_rotate 7
```

logformat : Nombre y especificaciones del formato de los log

acces_log : Directorio para guardar los log y el formato.

logfile_rotate : Días de registro que se guardan en cada archivo de log.

Miscelania:

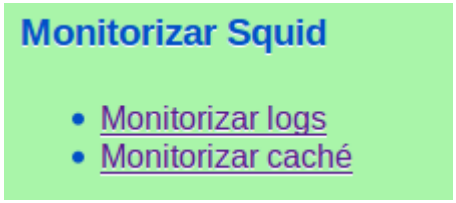
```
visible_hostname proxy_iesebre
dns_nameservers 192.168.202.1 192.168.203.1 192.168.204.1
```

visible_hostname : Nombre que se mostrará en los avisos del servidor

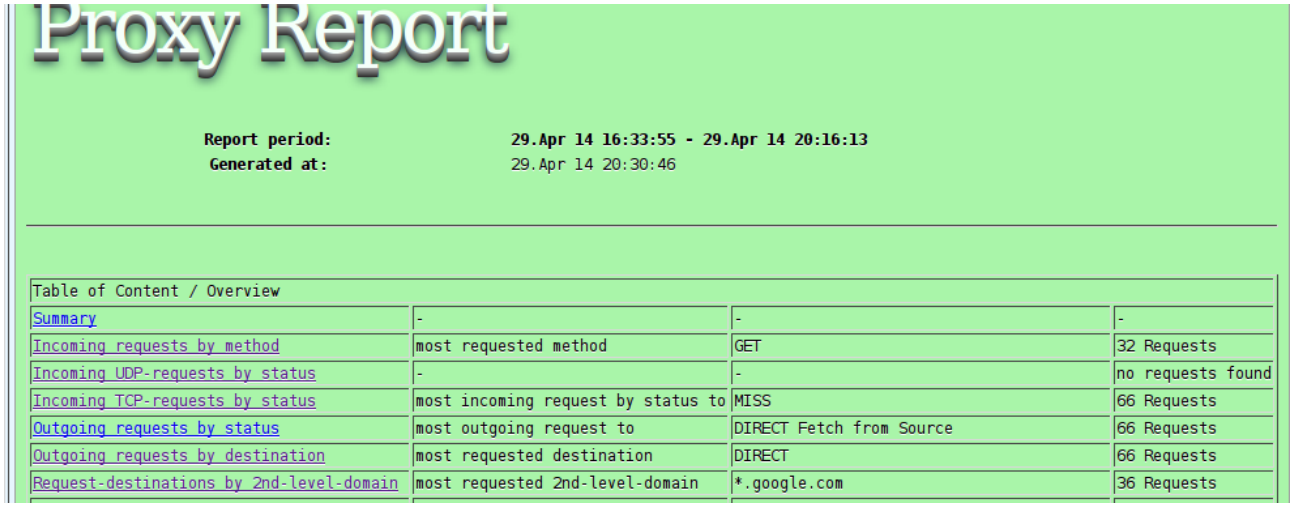
dns-nameservers : Servidores dns que utilizará squid.

3.1.1.2.Monitorizar Squid.

El entorno nos ofrece la posibilidad de realizar una monitorización del servidor Squid, podremos ver los logs del servidor, así como el uso que se hace de la caché.



Monitorizar los log : Nos mostrará el informe generado por ' calamaris ' en formato html en la pantalla principal.


Proxy Report
Report period: 29.Apr 14 16:33:55 - 29.Apr 14 20:16:13
Generated at: 29.Apr 14 20:30:46
Table of Content / Overview
Summary - - -
Incoming requests by method most requested method GET 32 Requests
Incoming UDP-requests by status - - no requests found
Incoming TCP-requests by status most incoming request by status to MISS 66 Requests
Outgoing requests by status most outgoing request to DIRECT Fetch from Source 66 Requests
Outgoing requests by destination most requested destination DIRECT 66 Requests
Request-destinations by 2nd-level-domain most requested 2nd-level-domain *.google.com 36 Requests

Monitorizar la caché : Podremos ver el uso que se hace de la caché del servidor en la pantalla principal mediante la herramienta ' cachemgr ' .

3.1.1.3.Restaurar archivos.

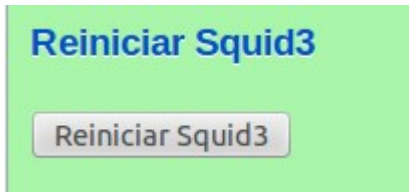
El entorno nos ofrece la posibilidad de restaurar los archivos que utiliza el servidor proxy.

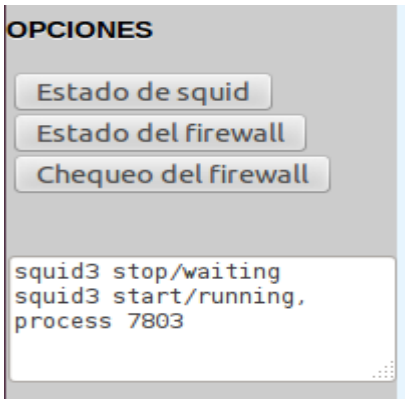
- **Restaurar archivo de config** : Este botón actúa sobre el archvo principal de configuración /etc/squid3/squid.conf. En caso de desastre, al pulsar el borón, se borra el archvo que haya actualmente y se restaura la copia que tenemos guardada en el directorio /etc/squid3/copias. Será necesario reiniciar el servidor para hecer efectivos los cambios.

- **Restaurar archivos de dominios y contenidos** : En este caso se actúa sobre las copias que se hayan guardado de los archivos de dominios y contenidos restringidos. En el caso de que no exista alguna copia de alguno de los 2 archivos se mostrará un error en la sección del menú lateral, es decir **es imprescindible** que haya una copia de ambos archivos para que se ejecute la restauración.

3.1.1.4.Reinicio del servicio.

En la parte inferior del menú de administración para el servidor proxy encontraremos un botón que nos permite reiniciar el servicio. Se nos mostrará un mensaje de aviso en el menú lateral.



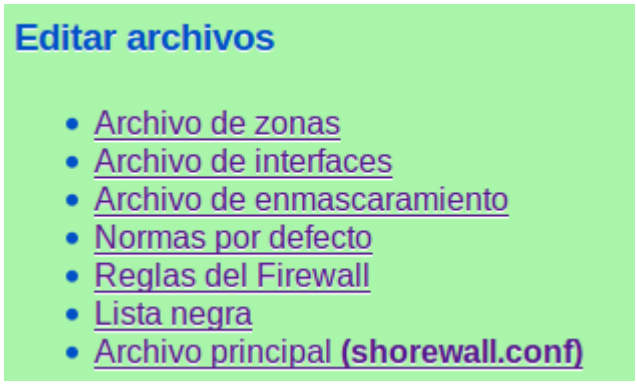


3.1.2.Opciones para el firewall Shorewall/Iptables.

Vamos a explicar todas las opciones que nos ofrece el menú de administración del firewall.

3.1.2.1.Edición de archivos.

En la parte superior encontraremos los enlaces correspondientes para poder editar todos los archivos que utilizará el firewall.



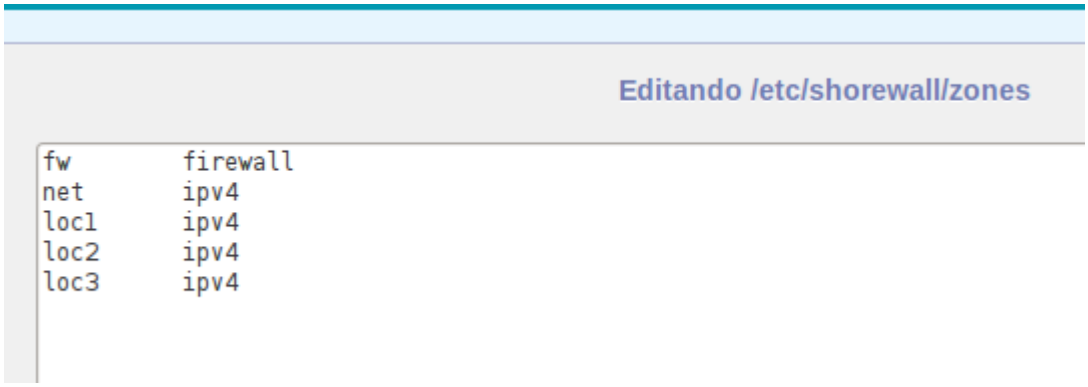
Nota: Los archivos de zonas,interfaces,enmascaramiento,normas por defecto y archivo principal, no deberían modificarse. Igualmente explicaremos la forma correcta de hacerlo.
La modificación de cualquiera de estos archivos, requiere reiniciar el firewall, para hecer efectivos los cambios.

Archivo de zonas:

La sintaxis del archivo es la siguiente:

Nombre de la zona Tipo de zona

Encontraremos las siguientes líneas:



fw : El propio servidor donde tenemos el firewall.

net : Será la interfaz que se uitiliza para acceder al router.

loc1 : La zona del aula 20.2.

loc2 : La zona del aula 20.3.

loc3: La zona del aula 20.4.

Tantas zonas como interfaces de red tenemos en el servidor.

Archivo interfaces:

En este archivo se asignan las interfaces del servidor a cada zona.

La sintaxis es la siguiente:

#Zone #Interface #Broadcast #Options

Zone: Nombre de la zona.

Interface : Interfaz de red que le asignamos.

Broadcast : Detección automática o no de la dirección de difusión.

Options : Diferentes opciones que podemos especificar de filtrado en cada interfaz, entre ellas:

tcpflags : Esta opción hace que Shorewall revise los paquetes por combinaciones ilegales de FLAGS (o banderas) TCP.

logmartians : Esta opción hace que Shorewall registre paquetes con direcciones de origen imposibles, para esto tenemos que tener habilitado el routefilter en la interfaz.

nosmurfs : Filtra paquetes smurfs (paquetes que tienen como dirección de origen una dirección de broadcast).

blacklist: Analiza los paquetes contra la lista negra en el archivo blacklist del shorewall.

routeback: Permite que Shorewall filtre paquetes que se devuelven a esta misma interfaz.

Teniendo en cuenta la configuración que tenemos realizada asignaremos las interfaces.

interfaces

```
auto lo
iface lo inet loopback

#Interfaz externa eth0
auto eth0
iface eth0 inet static
address 192.168.50.46
netmask 255.255.255.0
broadcast 192.168.50.255
gateway 192.168.50.1
dns-nameserver 127.0.0.1
dns-search www.iesebre.com

#Interfaz Aula 20.2
auto eth1
iface eth1 inet static
address 192.168.202.1
netmask 255.255.255.0
broadcast 192.168.202.255

#Interfaz Aula 20.3
auto eth2
iface eth2 inet static
address 192.168.203.1
netmask 255.255.255.0
broadcast 192.168.203.255

#Interfaz Aula 20.4
auto eth3
iface eth3 inet static
address 192.168.204.1
netmask 255.255.255.0
broadcast 192.168.204.255
```

Editando /etc/shorewall/interfaces

#ZONE	INTERFACE	BROADCAST	OPTIONS
net	eth0	detect	
loc1	eth1	detect	dhcp,blacklist
loc2	eth2	detect	dhcp,blacklist
loc3	eth3	detect	dhcp,blacklist

Notese que no hay asignación de interfaz a la zona del firewall(fw), logicamente es el propio servidor y contiene todas las interfaces de red.

Archivo de enmascaramiento:

Este archivo especifica que inetrfaz será enmascarada y la interfaz que lo hará posible. Es decir especifica la interfaz que ejecutará NAT *masquerade*.

La sintaxis es la siguiente:

#INTERFACE SOURCE ADDRESS PROTO PORT(S) IPSEC MARK USER/GROUP

Interface : Interfaz que realizará NAT masquerade.

Source : Interfaz de origen.

Se puede observar que existen varias opciones más que no vamos a utilizar. Si se desease información sobre el resto de opciones, mirar en el enlace:

http://shorewall.net/manpages/shorewall-masq.html

Como vemos la interfaz de salida eth0 del servidor es la que enmascara cada una de las interfaces que hemos asignado a cada aula.

Archivo de normas por defecto:

Archivo en el que se describen las acciones a realizar en el caso de no encontrar ninguna regla de firewall que se cumpla.

La sintaxis del mismo es la siguiente:

#SOURCE DEST POLICY LOG LEVEL LIMIT BURST CONNLIMIT MASK

Source : Nombre de la zona de origen de los paquetes.

Dest : Nombre de la zona de destino de los paquetes.

Policy : Acción que se debe ejecutar. Entre las más habituales:

Accept : Acepta los paquetes de la zona de origen a la de destino.

Reject : Rechaza los paquetes de la zona de origen a la de destino enviando un mensaje ICMP 'unrecheable'.

Drop : Ignora los paquetes de la zona de origen a la de destino

Log level : Realizar o no un registro del evento.

El resto de opciones no las emplearemos en este caso, podemos encontrar toda la información en el enlace:

http://shorewall.net/manpages/shorewall-policy.html

Editando /etc/shorewall/policy

```
#SOURCE     DEST    POLICY    LOG LEVEL    LIMIT BURST    CONNLIMIT MASK
fw          net     ACCEPT
net         all     REJECT        $LOG
all         all     DROP          $LOG
```

Se permite el paso de la zona del firewall al exterior.

Se rechaza el paso de la zona externa a cualquier zona realizando un registro.

Se ignoran los paquetes de cualquier zona de origen a cualquier zona de destino (CATCHUP) realizando un registro.

Archivo de reglas del firewall:

En este archivo se definen las reglas que permitirán o denegarán el paso de los paquetes a Ips, puertos, protocolos etc..

Nota: Las reglas se leen de arriba hacia abajo. Puesto que se solicita en modo restrictivo, las normas más restrictivas deberán situarse en la parte superior del archivo.

La sintaxis básica del mismo es la siguiente:

#ACTION SOURCE DEST PROTO DEST-PORT SOURCE-PORT

Action : Define la acción que haya que realizar. Entre ellas las más usadas:

Accept : Acepta los paquetes de la zona de origen a la de destino.

Reject : Rechaza los paquetes enviando un mensaje ICMP 'unrecheable'.

Drop : Ignora los paquetes.

Source : Nombre de la zona de origen de los paquetes.

Dest : Nombre de la zona de destino del paquete.

Proto : Protocolo que se utiliza en el envío del paquete.

Dest-port : Puerto de destino del paquete.

Source-port : Puerto de origen del paquete.

Existen más opciones y muy extensas que se pueden configurar, para ello recomiendo visitar el enlace:

http://shorewall.net/manpages/shorewall-rules.html

Editando /etc/shorewall/rules

```
ACCEPT  loc1    net:192.168.50.80       tcp
ACCEPT  loc2    net:192.168.50.80       tcp
ACCEPT  loc3    net:192.168.50.80       tcp
ACCEPT  loc1    fw      tcp     80,3128
ACCEPT  loc2    fw      tcp     80,3128
ACCEPT  loc3    fw      tcp     80,3128
Ping/ACCEPT     fw      all
Ping/ACCEPT     loc1    all
Ping/ACCEPT     loc2    all
Ping/ACCEPT     loc3    all
DNS/ACCEPT      loc1    fw
DNS/ACCEPT      loc2    fw
DNS/ACCEPT      loc3    fw
DHCPfwd/ACCEPT  loc1    fw
DHCPfwd/ACCEPT  loc2    fw
DHCPfwd/ACCEPT  loc3    fw
```

De abajo hacia arriba:

DHCPfwd/ACCEPT : Se permiten las peticiones DHCP de la zona de las 3 aulas al servidor.

DNS/ACCEPT : Se permiten las peticiones DNS de la zona de las 3 aulas al servidor.

Ping/ACCEPT : Se permite realizar ' ping ' desde la zona de las aulas y el servidor a cualquier destino.

ACCEPT locx fw tcp 80,3128 : Se permite el acceso de la zona de las aulas utilizando el protocolo tcp, cuyo puerto de destuino sea el 80 ó el 3128.

ACCEPT locx net:192.168.50.80 tcp : Se permite el acceso de la zona de las 3 aulas a la zona exterior, solo a la IP 192.168.50.80

Ejemplos de edición:

-Bloquear a un usuario concreto(192.168.202.228, aula 20.2) el acceso a la dirección 192.168.50.80

```
REJECT      loc1:192.168.202.228     net:192.168.50.80
```

-Bloquear a un usuario concreto el acceso a internet a través del proxy(esto lo haremos en el archivo blacklist).

```
REJECT    loc1:192.168.202.228     fw    tcp    3128
```

-Permitir el acceso a un profesor(192.168.20**x**.100) al exterior sin utilizar el proxy.

```
ACCEPT    locx:192.168.20x.100      net     all     all
```

Sustituiremos la ' **x** ' por el número final del aula al que corresponda.

-Permitir realizar conexiones externas SSH al aula 20.2.

```
ACCEPT    loc1    net     tcp    22
```

Archivo lista negra:

Archivo que utilizaremos para prohibir el acceso a una determinada dirección IP una red o rango de ellas, a un puerto o protocolo.

Sintaxis del archivo:

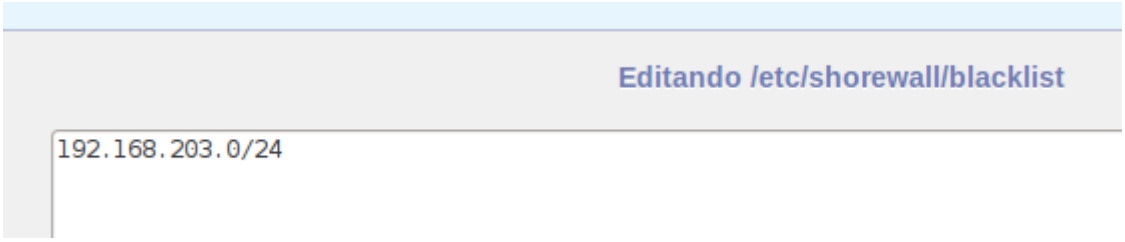
#ADDRESS/SUBNET PROTOCOL PORT

Address/subnet : Dirección Ip o de red y/o su máscara.

Protocol : Protocolo que queremos bloquear.

Port : Puerto que vamos a bloquear.

Simplemente se edita en modo de lista especificando la dirección que queremos bloquear o la red y podemos o no añadir, según se necesite, el protocolo y el puerto.



Aquí estaríamos bloqueando a todo el aula 20.3 todo tipo de acceso.

Podríamos añadir a la lista tan solo una serie de puertos y/o protocolos que queremos bloquear sin especificar direcciones IP.

Para más información:

http://shorewall.net/manpages/shorewall-blacklist.html

Archivo principal(shorewall.conf).

Archivo principal de configuración del firewall Shorewall/Iptables, que no debríamos tener que modificar.

Tan solo deberán estar activas las directivas :

STARTUP_ENABLED=Yes ==> Arranque de shorewall.

IP_FORWARDING=On ===> Permite el enrutamiento de paquetes para poder efectuar NAT *masquerade.*

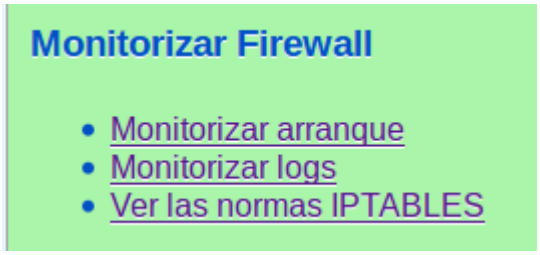
Resulta un archivo extenso con múltiples directivas en las que no voy a entrar a explicar una a una, pues no se trata de crear un manual de uso del Shorewall si no del uso del entorno de administración.

Para información detallada sobre las directivas de este archivo acudir al enlace:

http://shorewall.net/manpages/shorewall.conf.html

3.1.2.2.Monitorizar el Firewall.

El entorno de administración nos ofrece la posibilidad de realizar una monitorización del firewall a nivel de arranque, registros y visualizar las **normas** que ha creado **de filtro** en Iptables.

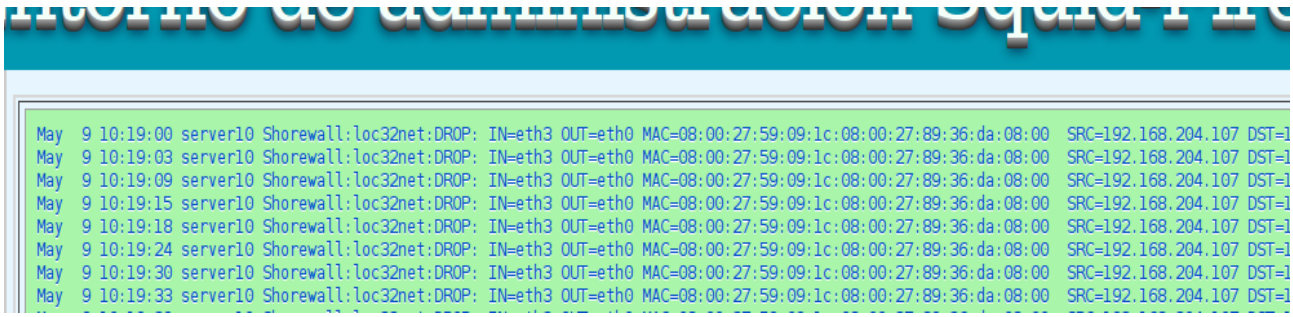


Monitorizar arranque:

Nos permite visualizar los sucesos en el inicio de Shorewall, donde podremos comprobar si todo ha ido bien o algo a fallado.

Monitorizar los log:

Al pulsar el botón se nos mostrará el archivo ,extenso y detallado, de los registros que va generando el firewall.



Ver normas de Iptables:

Al pulsar el botón nos mostrará las normas por defecto (filter) que hay creadas en Iptables, equivalente a ejecutar:

```
# iptables -L
```

Chain INPUT (policy DROP)
target prot opt source destination
dynamic all -- anywhere anywhere ctstate INVALID,NEW
net2fw all -- anywhere anywhere
loc12fw all -- anywhere anywhere
loc22fw all -- anywhere anywhere
loc32fw all -- anywhere anywhere
ACCEPT all -- anywhere anywhere
Drop all -- anywhere anywhere
ULOG all -- anywhere anywhere ULOG copy_range 0 nlgroup 1 prefix "Shorewall:
DROP all -- anywhere anywhere

3.1.2.3.Restauración de archivos.

En este caso solo existe una posibilidad:

- **Restaurar archivos** : Este botón actúa sobre todos los archivos del firewall. Elimina los antiguos y restaura las copias que tenemos guardadas en /etc/shorewall/copias.

Realizará una restauración de los archivos:

- *zones.*
- *interfaces.*
- *masq.*
- *policy.*
- *rules.*
- *blacklist.*
- *shorewall.conf.*

Será necesario reiniciar el servicio para activar los cambios.

Al terminar nos mostrará el mensaje correspondiente en la zona lateral del menú.

3.1.2.4.Reinicio del servicio.

En la parte inferior del menú de opciones del firewall veremos el botón correspondiente, para realizar el reinicio del servicio. Bastará pulsarlo para efectuar la acción y se nos mostrará el correspondiente mensaje en el lateral izquierdo donde podremos ver si ha funcionado bien.